January 2024 Issue

In this edition:

- DHS Releases Physical Security Performance Goals for Faith-Based Communities
- DHS CISA and UK NCSC Release Joint Guidelines for Secure AI System Development
- Expansion of the Secure Tomorrow Series Toolkit Now Available
- CISA Resources to Help Schools Strengthen Security and Build Resilience
- CISA Updates Toolkit to Promote Public Safety Communications and Cyber Resiliency
- CISA Announces Secure by Design Alert Series: How Vendor Decisions Can Reduce Harm at a Global Scale
- Cyber Education and Training Updates January 2024

Report a Cyber Incident

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities.

Report a Cybersecurity Incident: Report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870.

- Report an Incident
- Report Phishing
- Report a Vulnerability

Report incidents as defined by NIST Special Publication 800-61 Rev 2, to include

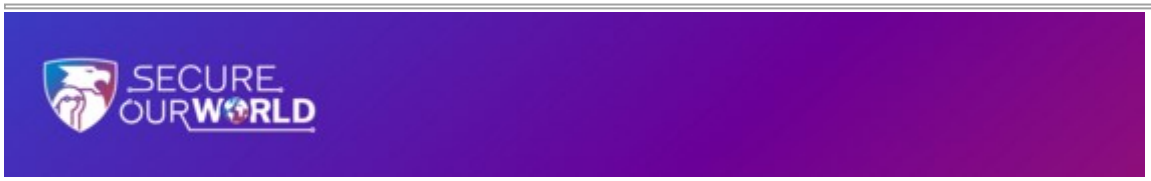
- Attempts to gain unauthorized access to a system or its data,
- Unwanted disruption or denial of service, or

- Abuse or misuse of a system or data in violation of policy.

Federal incident notification guidelines, including definitions and reporting timeframes can be found here.

Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to: **Central@CISA.dhs.gov**

Learn More Here



In 2024 Take Action Each Day to *Secure Our World*

CISA's New Cybersecurity Awareness Program Launched in September 2023 is Grabbing Attention

On September 26, 2023, CISA launched a new cybersecurity awareness program called Secure Our World. We are an increasingly connected world. Smart phones, laptops, tablets, smart home products and other connected devices are everywhere, and we use them for much of what we do. From arranging rides to and from airports, paying for meals, checking emails and texts, keeping an eye on our homes, and staying in touch with colleagues, friends, and loved ones, we stay connected and online constantly. At home and abroad, we rely on a safe and secure digital world, and we all must take steps every day to ensure we are safe online and when connected.

2024 is a perfect time to double-down on working together to drive behaviors that can significantly improve online safety and security, not only in the U.S., but throughout the world, wherever we are.

As cyber threats become more sophisticated, we all have an important role to play in keeping our digital world safe and secure. Working together, let us spread the word to give everyone the knowledge and tools they need to:

1. **Use strong passwords and a password manager**. Strong passwords mean long, random, and unique to each account. The easiest way to do this is by using a password manager to generate passwords and to save them.

2. **Turn on multifactor authentication** on all accounts that offer it. We need more than a password on our most important accounts, like email, financial accounts, online shopping, and of course social media.
3. **Recognize and report phishing**—as we like to say, think before you click. Be cautious of unsolicited emails or texts or calls asking you for personal information. Resist the urge to click on these links and do not click on links or open attachments from unknown sources.
4. **Update software**: In fact, enable automatic updates on software so the latest security patches keep devices we are connected to continuously up to date.

With CISA's new enduring program, Secure Our World, we are expanding our cybersecurity awareness focus beyond just Cybersecurity Awareness Month so that these mutually beneficial conversations will continue throughout the other 11 months of the year—conversations that empower individuals and families; small and medium-sized businesses; technology manufacturers; among others, to create new cyber secure habits that extend our lines of defense to our homes, our communities, our places of work, and everywhere in between.

For individuals and families, the Secure Our World program emphasizes the importance of securing personal accounts, offering guidance on personal device safety, safe internet browsing practices, social media usage, and protecting personal information online.

Because small and medium-sized businesses face unique challenges, we are working to help them Secure Our World by offering tools and resources that can help keep their businesses, employees, customers, and, ultimately, our communities safer.

Tech manufacturers can Secure Our World by implementing security features built-in by design. Default settings should automatically protect against the most prevalent threats and vulnerabilities, without end-users having to take additional steps. Individuals should manually bypass security features if they do not want them. Users should not have to opt-in for necessary security measures to make their products safe to use. Products should be safe for end users right out of the box.

To make it easy to get the word out, CISA released the first ever CISA Public Service Announcement and created a host of other easy to use resources. Many of these resources are offered in multiple languages and can be tailored for different international audiences.

CISA's foundation is built on a voluntary partnership model, and our partners mean everything to our mission and shared success. Please visit our webpage to find out more about becoming a partner. We look forward to working with you to Secure Our World year round.

Announcements, Opportunities and Resources

DHS Releases Physical Security Performance Goals for Faith-Based Communities

Learn More Here

Building on longstanding efforts and redoubling work to support faith-based communities in response to the ongoing conflict in the Middle East, the Department of Homeland Security (DHS), through Cybersecurity and Infrastructure Security Agency (CISA), released new resources to help houses of worship and other faith-based organizations enhance their security. These Physical Security Performance Goals – modeled after the successful Cybersecurity Performance Goals – are a collection of cost-effective actions specifically tailored for faith-based organizations that can be implemented to reduce risk without sacrificing accessibility. This is the latest resource the Biden-Harris Administration is offering to faith-based organizations in response to the current heightened threat environment.

“In this continued heightened threat environment, the Department of Homeland Security is committed to protecting every American’s right to live, express, and worship their faith freely and in safety,” **said Secretary of Homeland Security Alejandro N. Mayorkas.** “The physical security performance goals we are releasing, provide churches, synagogues, mosques, and other faith-based institutions with cost-effective, accessible, and readily implementable strategies to enhance their security and reduce the risk to their communities. I strongly urge all faith-based institutions to take advantage of this new resource and incorporate the security practices it outlines.”

“CISA remains fully committed to its longstanding partnership with faith-based leaders to advance the protection of houses of worship while preserving their open and welcoming environments,” **said CISA Director Jen Easterly**. “The agency has a long track record of supporting faith-based communities in improving physical and cyber security practices. These performance goals are the latest example.”

Because Houses of Worship are the center for regular faith-based services and gatherings across the country, they are vulnerable as potential targets for malicious actors. The Physical Security Performance Goals for Faith-Based Organizations establish a baseline set of security practices to help houses of worship plan for, protect against, and respond to threats. Understanding that all facilities are different, the goals allow organizations to create tailored, actionable plans that will address their specific needs and serve their community.

“While the threat environment continues to be challenging across all faiths, houses of worship and other faith-based organizations and people are often targets. Preparedness is key to mitigating risk,” **said Mayya Saab, Executive Director of the Faith-Based Information Sharing and Analysis Organization and DHS Faith-Based Security Advisory Council Member.** “The *Physical Security Performance Goals for Faith-Based Communities* resource provides a visual guide to a goal setting activity that can help houses of worship and faith-based organizations prioritize security goals based on understanding their unique risk. The guide will be especially helpful to less resourced houses of worship.”

“The Secure Community Network is proud to partner with the Department of Homeland Security to ensure the highest quality guidance for faith-based communities amidst a time of increased threat of hate and violence,” **said Michael Masters, Secure Community Network National Director & CEO and DHS Faith-Based Security Advisory Council Member.** “The opportunity to offer our organizational expertise throughout this process reflects the commitment of the Department and its leadership to ensure the safety and security of faith-based communities across the country. DHS guidance continues to set a high standard and example that our community is proud to follow, and we look forward to the work of our continued partnership.”

“This *Physical Security Performance Goals for Faith-Based Communities* is a clear, concise, and convenient tool that is outstanding for any religious organization seeking to establish performance goals and protocols for response,” **said Ako Cromwell, Director of Global Security, African Methodist Episcopal Church.** “While it is particularly useful for those of us in the faith-based community, the fundamentals delineated in this product are applicable across the spectrum for security professionals. As always, we are most grateful to President Biden, Secretary Mayorkas, and all our Department of Homeland Security partners for their tireless efforts to keep us informed and secure.”

“Threats to houses of worship in the United States are increasingly complex and widespread, ranging from domestic hate ideologies to challenges intensified by transnational repression and geopolitical events,” **said Sim J. Singh Attariwala, Senior Policy and Advocacy Manager of the Sikh Coalition.** “We maintain that the federal government plays a pivotal role in safeguarding our communities. This

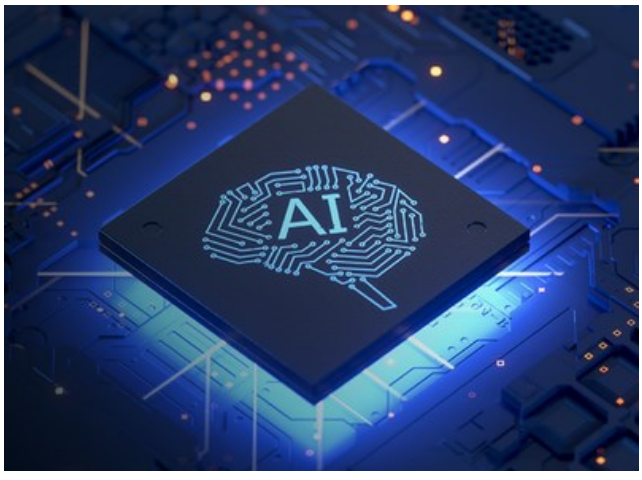
responsibility includes providing comprehensive and accessible resources, such as this document, to address both home-grown and international threats effectively.”

As the Israel-Hamas conflict has escalated, DHS has met with hundreds of community leaders in addition to coordinating with state and local enforcement and has disseminated Departmental resources to ensure faith-based communities can access available resources in one place. The Department continues to engage with communities through our Faith-Based Security Advisory Council and through the Protecting Places of Worship initiative, an effort co-led by DHS, the Department of Justice and the White House Office of Faith-Based and Neighborhood Partnerships. Through CISA’s regional security advisors, the Department also provides resources such as conducting assistance visits, vulnerability assessments, providing training, security and threat awareness and help to develop drills and exercises. Additionally, through the Department’s CP3 regional prevention coordinators, the Department shares information with community leaders on how to prevent acts of violence at the earliest possible stage.

In recent years, CISA has significantly increased its regional presence to meet the needs of stakeholders, including in faith-based communities, and regularly conducts extensive outreach to raise awareness of the available tools and resources that CISA makes available. You can read more about CISA's support to faith-based communities on CISA.gov.

Learn More Here

CISA and UK NCSC Release Joint Guidelines for Secure AI System Development



Taking a significant step forward in addressing the intersection of artificial intelligence (AI) and cybersecurity, CISA and the United Kingdom’s National Cyber Security Centre (NCSC) jointly released *Guidelines for Secure AI System Development* to help developers of any systems that use AI make informed cybersecurity decisions at every stage of the development process. The guidelines were formulated in cooperation with 21 other agencies and ministries from

across the world – including all members of the Group of 7 major industrial economies -- and are the first of their kind to be agreed to globally.

“We are at an inflection point in the development of artificial intelligence, which may well be the most consequential technology of our time. Cybersecurity is key to building AI systems that are safe, secure, and trustworthy,” **said Secretary of Homeland Security Alejandro N. Mayorkas.** “The guidelines jointly issued by CISA, NCSC, and our other international partners, provide a commonsense path to designing, developing, deploying, and operating AI with cybersecurity at its core. By integrating ‘secure by design’ principles, these guidelines represent an historic agreement that developers must invest in, protecting customers at each step of a system’s design and development. Through global action like these guidelines, we can lead the world in harnessing the benefits while addressing the potential harms of this pioneering technology.”

The guidelines provide essential recommendations for AI system development and emphasize the importance of adhering to Secure by Design principles that CISA has long championed.

“The release of the Guidelines for Secure AI System Development marks a key milestone in our collective commitment—by governments across the world—to ensure the development and deployment of artificial intelligence capabilities that are secure by design,” **said CISA Director Jen Easterly**. “As nations and organizations embrace the transformative power of AI, this international collaboration, led by CISA and NCSC, underscores the global dedication to fostering transparency, accountability, and secure practices. The domestic and international unity in advancing secure by design principles and cultivating a resilient foundation for the safe development of AI systems worldwide could not come at a more important time in our shared technology revolution. This joint effort reaffirms our mission to protect critical infrastructure and reinforces the importance of international partnership in securing our digital future.”

The guidelines are broken down into four key areas within the AI system development lifecycle: secure design, secure development, secure deployment, and secure operation and maintenance. Each section highlights considerations and mitigations that will help reduce the cybersecurity risk to an organizational AI system development process.

“We know that AI is developing at a phenomenal pace and there is a need for concerted international action, across governments and industry, to keep up,” **said NCSC CEO Lindy Cameron**. “These Guidelines mark a significant step in shaping a truly global, common understanding of the cyber risks and mitigation strategies around AI to ensure that security is not a postscript to development but a core requirement throughout. I’m proud that the NCSC is leading crucial efforts to raise the AI cyber

security bar: a more secure global cyber space will help us all to safely and confidently realize this technology's wonderful opportunities."

"I believe the UK is an international standard bearer on the safe use of AI," said **UK Secretary of State for Science, Innovation and Technology Michelle Donelan**. "The NCSC's publication of these new guidelines will put cyber security at the heart of AI development at every stage so protecting against risk is considered throughout."

These guidelines are the latest effort across the U.S.'s body of work supporting safe and secure AI technology development and deployment. In October, President Biden issued an Executive Order that directed DHS to promote the adoption of AI safety standards globally, protect U.S. networks and critical infrastructure, reduce the risks that AI can be used to create weapons of mass destruction, combat AI-related intellectual property theft, and help the United States attract and retain skilled talent, among other missions.

Earlier this month, CISA released its Roadmap for Artificial Intelligence, a whole-of-agency plan aligned with national strategy to address our efforts to promote the beneficial uses of AI to enhance cybersecurity capabilities, ensure AI systems are protected from cyber-based threats, and deter the malicious use of AI capabilities to threaten the critical infrastructure Americans rely on every day. Learn more about CISA's AI work.

Learn More Here

Expansion of the Secure Tomorrow Series Toolkit Now Available

"Resolve to be Resilient" - New interactive products for stakeholders

CISA has released the latest **Secure Tomorrow Series Toolkit**, a diverse array of interactive products to empower critical infrastructure stakeholders on how to use strategic foresight methods to identify and mitigate emerging risks.

After the successful launch of the first iteration of the Secure Tomorrow Series Toolkit in 2022, CISA expanded the Toolkit by adding three new risk topics: brain-computer interfaces, synthetic biology, and quantum technologies. The Toolkit is a diverse array of interactive and thought-provoking products designed to assist critical infrastructure stakeholders understand how to use strategic foresight methods to identify emerging risks and potential risk management strategies to secure critical infrastructure systems in the long-term.

The Secure Tomorrow Series is a strategic foresight capability focused on anticipating future risk drivers, critical uncertainties, and trends—such as aging infrastructure, global pandemics, and emerging technologies— to help enhanced organizational resiliency to be robust against future uncertainties. Central to the effort is the selection of topics likely to have highly disruptive impact to multiple National Critical Functions (NCFs) in the next 3 to 7 years.

To build the Toolkit, CISA engaged with subject matter experts, thought leaders, academia, think tanks, the private sector, and the National Labs to examine three new topics: brain-computer interfaces (BCI), synthetic biology, and quantum technologies. The first edition of the Toolkit (available on the Secure Tomorrow Series webpage) addresses three additional topics: trust and social cohesion, anonymity and privacy, and data storage and transmission. The Toolkit includes game templates, facilitator, and player guides, read-a-heads, and other materials uniquely designed to allow users to self-facilitate and conduct different kinds of strategic foresight activities around these topics that are relevant to their organization, region, or sector.

In a constantly changing and complex operating environment, using strategic foresight to explore alternative futures and potential drivers of change is a potent technique for improving decision-making to manage uncertainty.

Download/share the Secure Tomorrow Series Toolkit.

To learn more, visit the Secure Tomorrow Series webpage.

Learn More Here

CISA Resources to Help Schools Strengthen Security and Build Resilience

Schools provide the foundation for our nation's future success and are an essential component of our everyday lives, providing services to millions of children, families, and communities across the country. K-12 schools are also part of our nation's critical infrastructure. To ensure the safety and wellbeing of students, educators, and staff, schools must be aware of risks and threats, create and implement actionable security plans, and be able to withstand and recover from incidents. Critical Infrastructure Security and Resilience Month, observed in November, is an annual effort led by the CISA and focuses on educating and engaging all levels of government, infrastructure owners and operators, and the American public about the vital role critical infrastructure plays in the nation's wellbeing and why it is important to strengthen critical infrastructure security and resilience.

Recently we've witnessed increased frequency and intensity of threats and hazards facing our critical infrastructure, from natural disasters to targeted violence to cyberattacks. This year, CISA asks everyone, including the education community, to Resolve to be Resilient by preparing for and investing in resilience today, so we can withstand or recover quickly in the event of an incident tomorrow.

CISA takes seriously our commitment to school safety and supports K-12 schools and districts in their efforts to enhance school security and build resilience. Together with our Federal agency and non-government partners, we develop actionable guidance, evidence-based practices, tools, and more to help educate, equip, and empower school leaders to foster change and be better prepared for an evolving threat environment.

Some of the ways schools can build resilience through CISA resources include:

- **Take steps in advance to prevent potential incidents**. CISA partnered with the U.S. Secret Service National Threat Assessment Center to develop the K-12 Bystander Reporting Toolkit, which offers simple strategies and guidance K-12 schools and school districts can use to implement and enhance safety reporting programs.
- **Assess risks and their potential impacts**. CISA created the K-12 School Security Guide Product Suite to provide K-12 districts and campuses with resources, tools, and strategies to evaluate vulnerabilities, strengthen security, and better protect school communities.
- **Examine and test safety processes and plans through exercises**. CISA Tabletop Exercise Packages are a comprehensive set of resources designed to assist schools and districts in conducting their own exercises and initiating discussions within their organizations about their ability to address a variety of threat scenarios.
- **Address systemic cybersecurity risk**. CISA's Cybersecurity for K-12 Education provides tools, information, and resources to protect against attacks by malicious cyber actors and reduce the likelihood of successful cyber incursions.
- **Develop sustainable capabilities to address an evolving threat environment**. CISA's regionally based security advisors assess, advise, and assist and provide a variety of risk management and response services.
- **Create holistic school safety plans**. CISA administers SchoolSafety.gov. a Federal interagency website that provides a one-stop access point to school safety information, resources, and tools on a range of topics and threats.

For more information and helpful resources for the school safety community, visit CISA's School Safety page.

Learn More Here

CISA Updates Toolkit to Promote Public Safety Communications and Cyber Resiliency

CISA collaborates with public safety, national security, and emergency preparedness communities to enhance seamless and secure communications to keep America safe, secure, and resilient. Any interruption in communications can have a cascading effect, impacting a public safety agency's ability to deliver critical lifesaving services to the community. Therefore, public safety agencies carefully plan, implement, and review communications capabilities for resiliency to maintain daily communications abilities and prepare in advance for emergency events.

To assist public safety agencies in navigating the wealth of information available regarding communications resiliency, CISA created the *Public Safety Communications and Cyber Resiliency Toolkit* to identify and address emergent trends and issues, consolidate resources, educate stakeholders at all levels of government, and propose mitigations to enable resilient public safety communications. The Toolkit is designed to assist public safety agencies and others responsible for communications networks by providing the tools necessary to evaluate current resiliency capabilities, identify ways to improve resiliency, and develop plans for mitigating the effects of potential resiliency threats.

Using an interactive graphic displaying components of the emergency communications ecosystem, Toolkit users can easily navigate through several of topics and access applicable resources. Current topic areas include:

- Alerts, Warnings, and Notifications
- Cyber Incidents
- Cybersecurity
- Electromagnetic Pulse (EMP)
- Jamming
- Land Mobile Radio (LMR)
- Local Access Networks (LAN)
- Next Generation 911 (NG911)
- Positioning, Navigation, and Timing (PNT) Disruptions
- Power
- Priority Services

- Ransomware
- Resiliency Introduction
- Site Hardening
- Unmanned Aircraft Systems (UAS)

As part of CISA's commitment to provide the most up-to-date information in support of communications and cyber resiliency, the Toolkit is designed to be a living document, with the ability to grow and expand as new resources are developed and identified. Since its last update in December 2022, the Toolkit has been updated with 11 new resources spread over the existing sections. Users are encouraged to revisit the Toolkit on a regular basis to take advantage of recently added information and resources. Check out the updates at https://www.cisa.gov/publication/communications-resiliency today!

For more information and additional guidance regarding communications resiliency, visit https://www.cisa.gov/safecom/technology.

Learn More Here

CISA Announces Secure by Design Alert Series: How Vendor Decisions Can Reduce Harm at a Global Scale

CISA leads the national effort to *understand*, *manage*, and *reduce* risk to our cyber and physical infrastructure. We continuously publish alerts and advisories to help defenders prioritize their work based on the current threats and software vulnerabilities. We additionally provide defenders with ongoing help prioritizing their scarce resources; for example, our Known Exploited Vulnerabilities (KEV) program identifies the common vulnerabilities and exposures (CVEs) that malicious actors are actively exploiting in the wild.

But to *reduce* the nation's risk, we need to do more than warn defenders about the most current attacks and software vulnerabilities. We need to look much further "left-of-boom" and into the software development practices fixing things before intrusions cause harm to the American people. We need to identify the recurring classes of

defects that software manufacturers must address by performing a root cause analysis and then making systemic changes to eliminate those classes of vulnerability. We need to spot the ways in which customers routinely miss opportunities to deploy software products with the correct settings to reduce the likelihood of compromise. Such recurring patterns should lead to improvements in the product that make secure settings the default, not stronger advice to customers in "hardening guides".

Most importantly, we need to convey that insecure technology products are not an issue of academic concern: they are directly harming critical infrastructure, small businesses, local communities, and American families. CISA is launching a new series of products: **Secure by Design Alerts**. When we see a vulnerability or intrusion campaign that could have been reasonably avoided if the software manufacturer had aligned to secure by design principles, we'll call it out. Our goal isn't to cast blame on specific vendors; to the contrary, we know that vendors make software development and security choices as part of broader business decisions. Instead, our goal is to shine a light on real harm occurring due to these "anti-security" decisions. While the usual dialogue around an intrusion is about how victims could have done more to prevent or respond, alerts in this new series will invert this dialogue by focusing attention on how vendor decisions can reduce harm at a global scale.

Our first publication in the Secure by Design Alert series focuses on malicious cyber activity against web management interfaces. It brings attention to how customers would be better shielded from malicious cyber activity targeting these systems if manufacturers implemented security best practices and eliminated repeat classes of vulnerabilities in their products – and aligned their work to Secure by Design principles.

One of the core principles we identified in our Secure by Design whitepaper is to "take ownership for customer security outcomes". By identifying the common patterns in software design and configuration that frequently lead to customer organizations being compromised, we hope to put a spotlight on areas that need urgent attention. The journey to build products that are secure by design is not simple and will take time. We hope Secure by Design Alerts will help software manufacturers evaluate their software development lifecycles and how they relate to customer security outcomes.

Learn More Here

Cyber Education & Training Updates

January 2024

Highlights: What You Want to Know

The CYBER.ORG Range celebrates its one-year anniversary! Made possible with initial funding from the state of Louisiana and expanded by CISA, the Range has been leveraged by over 2,000 teachers in high school classrooms and over 30,000 student accounts from all 50 states in just one year. CYBER.ORG Range differs from other industry ranges, as it makes learning cybersecurity easier for teachers and students alike who want to increase their confidence in cyber education and explore the field. The Range is also available for students who have had no prior knowledge in cybersecurity. Learn more at https://cyber.org/news/happy-birthday-cyberorg-range-celebrating-one-year-and-reaching-all-50-states

Two courses were added to the Federal Virtual Training Environment (FedVTE), for the **Cyber Defense Analyst** and the **Cyber Defense Infrastructure Support Specialist**. Each new course is mapped to the NICE Framework, and each features guided labs from subject matter experts demonstrating the skills necessary to succeed in these two roles.

Incident Response (IR): This free training series includes 100-level webinars for a general audience which are cybersecurity topic overviews that provide core guidance and best practices to make your network more resilient to attacks. It also includes 200-level Cyber Range Training courses for government employees and contractors across federal, state, local, tribal, and territorial government, educational partners, and critical infrastructure partners. These Cyber Range Trainings provide guided step-action labs to learn and practice investigation, remediation, and incident response skills.

IR Training Events through January 2024

Date	Course Code	Registration Opens	Course	Hours
01/11/2024	IR110	11/16/2023	**Introduction to Log Management Webinar**	1

To learn more or register visit**: https://www.cisa.gov/resources-tools/programs/Incident-Response-Training**

Industrial Control Systems (ICS): We offer free, virtual ICS trainings geared toward Critical Infrastructure owners and operators. The trainings are designed to reduce cybersecurity risks to critical infrastructure and encourage cooperation between CISA and the private sector. Trainings vary in length and run from 8:00 a.m. – 5:00 p.m. MST (10:00 a.m. – 7:00 p.m. EST). All trainings are conducted through Online Training or CISA Virtual Learning Portal (VLP), with the exception of

the three- or four-day, in-person courses at Idaho National Labs (INL) in Idaho Falls, ID.

ICS Training Events through January 2024

Date	Course Code	Course	Location
01/08/2024-01/26/2024	**401v**	**Industrial Control Systems Evaluation (401v)**	**Scheduled Online Training**
01/08/2024-01/26/2024	**301v**	**Industrial Control Systems Cybersecurity (301v)**	**Scheduled Online Training**
01/29/2024-02/01/2024	**301L**	**Industrial Control Systems Cybersecurity Training – In-Person 4 Days**	**IN-PERSON TRAINING (4 days)**
On Demand	**100W**	**Operational Security (OPSEC) for Control Systems**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-1**	**Differences in Deployments of ICS**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-2**	**Influence of Common IT Components on ICS**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-3**	**Common ICS Components**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-4**	**Cybersecurity within IT & ICS Domains**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-5**	**Cybersecurity Risk**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-6**	**Current Trends (Threat)**	**CISA Training Virtual Learning Portal (VLP)**

On Demand	**210W-7**	**Current Trends (Vulnerabilities)**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-8**	**Determining the Impacts of a Cybersecurity Incident**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-9**	**Attack Methodologies in IT & ICS**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-10**	**Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**210W-11**	**Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2**	**CISA Training Virtual Learning Portal (VLP)**
On Demand	**FRE2115**	**Industrial Control Systems Cybersecurity Landscape for Managers**	**CISA Training Virtual Learning Portal (VLP)**

To learn more or sign up, visit: **https://www.cisa.gov/ics-training-calendar**

**The following virtual courses are prerequisites to attending in-person 301 and 401 trainings hosted by CISA at the Idaho National Laboratory:*

- *ICS 301v: Focuses on understanding, protecting, and securing ICS from cyberattacks.*
- *ICS 401v: Focuses on analyzing and evaluating an ICS network to determine its defense status and what changes need to be made.*

CyberWarrior's Master Class: The CISA Cyber Workforce Development and Training for Underserved Communities program increases opportunity and economic mobility for people of all backgrounds through training, mentorship and technology. Our program partners at the CyberWarrior Academy, deliver hands-on, intensive, lab-driven technical training in cybersecurity methods and procedures.

CyberWarrior Training Events

Date Audience Course

01/11/2024	**General Public**	**January Master Class – Introduction to Cybersecurity**

To learn more or sign up, visit: **https://www.cyberwarrior.com/cybersecurity-events/**

CISA's K – 12 Cybersecurity Education Training Assistance Program (CETAP): Through CETAP grantee, we offer K-12 teachers with cybersecurity curricula and education tools. CYBER.ORG develops and distributes cybersecurity, STEM and computer science curricula at no cost to K-12 educators across the country. Below are upcoming training events through CYBER.ORG.

CYBER.ORG Training Events through January 2024

Date	Audience	Course
09/01/2023-08/31/2024	**K-8 Educators**	**K-8 Cybersecurity Teachers Cohort, 2023-2024 School Year:** Are you a K-8 educator teaching cybersecurity in a classroom this 2023-2024 school year? Come exchange ideas with other teachers across the U.S.! K-8 Cybersecurity Teachers Cohort 2023-2024 | CYBER.org
09/01/2023-08/31/2024	**High School Educators**	**High School Cybersecurity Teachers Cohort, 2023-2024 School Year:** Are you an educator teaching cybersecurity in a high school classroom this 2023-2024 school year? Come exchange ideas with fellow U.S. educators! High School Cybersecurity Teachers Cohort 2023-2024 | CYBER.org
09/01/2023-08/31/2024	**K-12 Educators**	**CYBER.ORG Range Teachers Cohort, 2023-2024 School Year:** Are you an educator using the Cyber Range during the 2023-2024 school year? Come exchange ideas with fellow U.S. educators doing the same! CYBER.ORG Range Teachers Cohort 2023-2024 | CYBER.org

To learn more or sign up, visit: **https://cyber.org/events**

Federal Cyber Defense Skilling Academy: The Federal Cyber Defense Skilling Academy helps civilian federal employees develop their cyber defense skills through training in the baseline knowledge, skills, and abilities of a Cyber Defense Analyst (CDA). Students will have the opportunity to temporarily step away from their current role while they participate in the intense, full-time, three-month accelerated training program. Below are the Skilling Academy cohort dates for FY24:

Skilling Academy Program Dates through 2024

Academy	Program Start/End Date	Applications Open	Applications Close
7 and 8	**03/04/24 – 06/14/24**	**12/18/2023**	**01/11/2024**
9 and 10	**04/01/24 – 07/12/24**	**01/22/2024**	**02/08/2024**
11 and 12	**05/06/24 – 08/16/24**	**02/19/2024**	**03/07/2024**

To learn more or register, visit**:** **https://www.cisa.gov/SkillingAcademy**

Continuous Diagnostics and Mitigation (CDM): We offer instructor led, hands-on CDM Dashboard training for U.S. Executive Branch employees and contractors in our virtual cyber range training environment. These courses are intended for those at agencies participating in the CDM program who monitor, manage and/or oversee controls on their information systems (e.g., ISSOs, CDM POCs, ISSMs and those who report metrics and measures).

The CDM training goal is to provide the learner the basics of CDM and using the CDM Dashboard capabilities to help mitigate agency threats. We will also provide numerous CDM resources and external references.

All courses will be taught utilizing the latest version of the CDM Dashboard (ES-6.0.5) within a cyber virtual training range (CVLE). The course content has been updated and will focus on the current version ES-6 of the CDM Dashboard, including the latest dashboard content pack, version 6.0.5. The latest CDM

Dashboard capabilities will be discussed, including FISMA Automation. The current CDM courses fall into the 100 level (Introductory) and 200 level (Intermediate) level offerings.

CDM Training Events through January 2024

Date	Course Code	Registration Opens	Course	Hours
01/04/2024	**CDM210**	**11/22/2023**	**CDM Enabled Threat Hunting (CETH) using the CDM Dashboard**	4
01/09/2024	**CDM320**	**11/27/2023**	**Using the CDM Dashboard to Respond to Federal Mandates and BOD 22-01 and BOD 23-01**	4
01/18/2024	**CDM301**	**11/30/2023**	**Management Overview of CDM and the CDM Agency Dashboard**	2
01/23/2024	**CDM141**	**12/5/2023**	**Introduction to the CDM Agency Dashboard**	4
01/30/2024	**CDM143**	**12/12/2023**	**Vulnerability Management using the CDM Agency Dashboard**	4

To learn more or register visit: **https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-training**

Contact Us: *Education@cisa.dhs.gov*

Want to subscribe? Sign up a co-worker or friend?

Email education@cisa.dhs.gov to receive this Cyber Training Bulletin each month!

Learn More Here

The CISA Community Bulletin is a monthly publication that shares webinars and workshops, new publications, and best practices.

To access past editions of this CISA Community Bulletin, please visit the CISA Community Bulletin Archive.